Update on Internet Identity and Collaboration Support

Ken Klingenstein, kjk@internet2.edu

Topics

- Identity
  - Federal, international and standards
  - InCommon and eduGAIN
  - Social Identities
  - Attribute release and consent
  - Federated incident handling
  - ORCID identifiers
- Access control and Collaboration Support
  - Scalable Attribute-based Access Control
  - Collaboration Platforms
- Agency takeaways
  - Gravitational waves as a use case
    - Increasing security, reducing barriers
  - Collaboration support checklist

National level initiatives

- Standards dev orgs
  - Kantara – new leadership, new roles
    - Likely home for interop, gov
  - IETF – fundamental protocols (OAuth, PKI, etc.)
  - OASIS – Syntax and semantics of domain XML
- FICAM, NSTIC and IDESG
- European General Data Protection Regulation (GDPR)

INTERNET 2

FICAM, NSTIC and IDESG

- FICAM continues, serving gov-gov and biz-gov
  - PKI Bridge provides high assurance, pharma, mechanisms for controlled substances
  - Large SAML federations, e.g. NIEF, serve law enforcement, health, justice, etc.
- NSTIC, initiated by Obama, has been enfolded into NIST
  - Pilots in specific niches, from innovative business plans to privacy and consent; varying success, winding down
  - IDESG to shape rules of the road for the identity ecosystem
- IDESG
  - Intent to create trust frameworks, schema, certifications for IdP, RP, intermediaries, etc.
  - After much effort, has produced an initial trust framework and an associated self-asserted listing service for interested parties

INTERNET 2

General Data Protection Regulation - GDPR

- Applies to all EU states
- Applies to all entities worldwide that have EU customers or clients (!) – includes EU citizens accessing US facilities
- Potentially massive fines (4% of global revenue)
- Revocable consent
- “Clearly” informed consent
- Right to be forgotten
- Right to data portability between IdP’s
- Sets age of consent from 13 to 16 (allows local exceptions)

Some implications

- Cloud-based data processors share responsibilities with data controllers (e.g. VM providers may need to know what's in the VM); 72 hour breach notification to authorities
- BAE++ (back-end contracts need to be approved by data controller)
- Implementing "clearly" informed, revocable, fine-grain consent
- Implementing the right to be forgotten
  - Managing backups and use of metadata
- Risk based requirements on companies to perform data protection assessments on full data life-cycle
- Almost one-stop shopping for multi-jurisdictional resolutions
- Data Protection Officers (~CPO) required with SME (small to medium enterprise) exceptions
- PrivacyShield (Safe Harbor 2.0) proposed but not yet approved

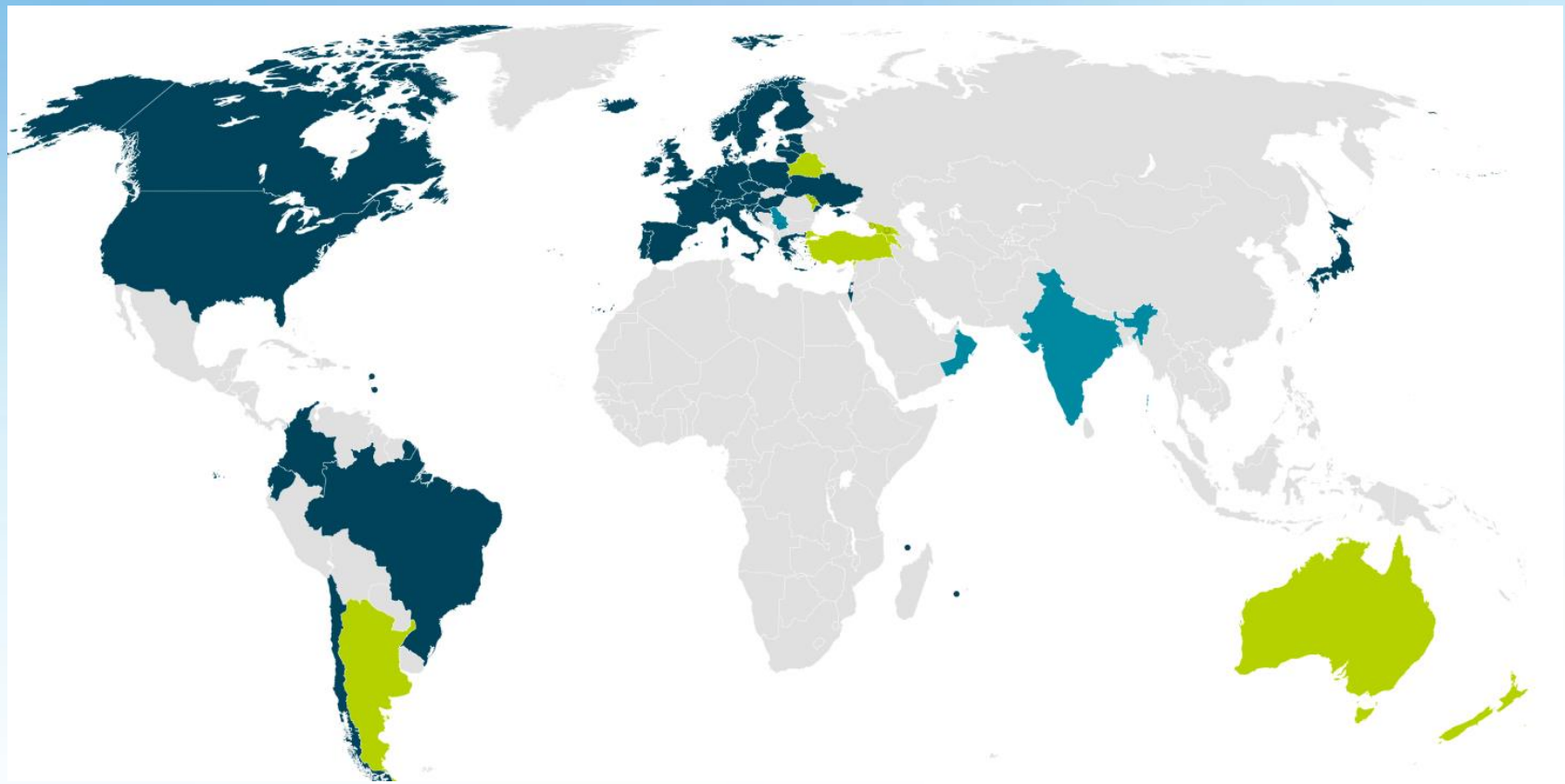
INTERNET 2

InCommon

- 842 + participants, essentially all academic research institutions
- >8 M users
- Hundreds of service providers, from Azure to AWS, Elsevier and IEEE, Microsoft to Box, Argonne to Pacific Northwest Labs to Woods Hole
- Certificate services important; MFA devices and licenses growing value
- MFA use on campuses is increasing significantly
- Important interop profiles emerging for inter-federation and MFA
  - https://spaces.internet2.edu/display/FIWG
  - https://spaces.internet2.edu/display/MIPWG
- Metrics for both InCommon and MFA need to change from number of participants to intensity of participation per member
  - E.g. number of relying parties per IdP, number of critical apps protected by MFA

INTERNET 2

Edugain membership



InCommon and eduGAIN

- InCommon has joined eduGAIN – interfederation is real
  - 41 National R&E federations in eduGAIN
  - > 31 M users and growing
  - Number of available IdP's for InCommon SP's has gone from 400 to 3000
  - NIH is already using several international partners for NIAIDS
- Very successful, but stresses in the system
  - Size of metadata bundle - moving to dynamic metadata (MDQ)
  - Semantics across national borders
  - Data movement across national borders

INTERNET 2

Social identities

- Increasingly integrated into the landscape
  - In protocol – e.g. Shib IdP v3 extension that issues OpenIdConnect tokens
  - In identities – e.g Social2SAML gateways that expands campus user base to students' parents, contractors, alumni, etc.
  - In services – IdP's who support multiple protocols such as UnitedId
- Exposes next sets of issues
  - Strength of identity proofing for social accounts
  - LOA, filtering out attributes
  - Data sovereignty concerns

INTERNET 2

Attribute release and consent management

- Attribute release is the single highest barrier to use
- Key dimension of privacy
- Complex set of legal and technical and international and financial and … issues
  - When and where and how to use is endless discussion
  - Initial and downstream are separate but very related topics
- Requirements list grows – informed, revocable, accessible, etc.
- Particularly challenging is selective release of values from a multivalued attribute (e.g. group memberships)
- R&S end-entity tag, trust marks, and end-user consent management all attempts to reduce the friction

INTERNET 2

Federated incident handling

- Concerns of major science service providers that if they go the federated route, they will be notified by IdP's of compromised accounts and other identity related events relevant to the service provider.
- SIRTIFI initiative out of CERN working with major labs and science facilities to define requirements
- Moving into broader circles of interest via Kantara
- Id-event activity in IDESG aligns well with standards on formats and protocols to move incident data around
  - Still early drafts, but promising
- May well become part of composable trust frameworks
  - E.g. InCommon + R&S + Edugain + SirTiFI

INTERNET 2

SirTiFi trust framework

- Who to expect in the EmailAddress tag?
- An individual or generic contact in the entity organisation's security team who has agreed to adopt the Sirtfi Framework
- This contact will:
  - Respect the Traffic Light Protocol (TLP) and confidentiality
  - Promptly (within one business day) acknowledges receipt of the security incident report
  - As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible
  - Respond to the incident reporter and any other impacted parties when the incident is resolved

INTERNET 2

ORCID identifiers

- A persistent unique scholarly identifier, intended to connect a researcher as they change institutions and affiliations
- Increasingly used by publishers, campus academic profile software, VIVO, research agencies, academic workflow, intermediaries
- Users can acquire them freely from orcid.org
- Provides possible opportunities for other purposes, such as account linking, but not without peril

INTERNET 2

Access Control and Collaboration Support

- Scalable Access Control
  - Using attributes of users, more than names of users, for access control
  - ACL's by group membership, role, citizenship, clearance, etc.
  - Increases security, scalability, end-user management, privacy
- Collaboration Support
  - Integrated identity management across the set of applications a VO uses – domain and collaborative
  - Participant life-cycle management
  - Privacy-preserving as appropriate
  - Leverage identity and security infrastructures

INTERNET 2

Collaboration Support

- Platforms
  - Software that provides identity and group membership information via open protocols to a set of collaboration applications
  - Apps can include: wikis, listprocs, Google Docs, github, jira, doodle, file transfers, video tools, audio tools, domain specific apps such as Globus and iRODS, resources such as Azure and AWS, etc
  - Examples include COmanage, Globus Nexus, Google+
- Deployment models
  - By a VO using VM's
  - By a local infrastructure – campus, lab
  - By a national or trans-national infrastructure – GEANT, SURFnet, JISC
    - Geant is offering collaboration as a service to all European VO's

INTERNET 2

Gravitational Waves and Collaboration

- LIGO, discoverers of Gravitational Waves, early adopters of Comanage (deployed by VO)
- Increasing security
  - Use of federated identity globally
  - Use of MFA
  - Highly managed access controls
  - Managed use of social identity
- Reducing friction
  - Use of federated identity globally
  - Automated life-cycle management of participation
  - Facile group management tools, include end-user controls, sensitivity controls, historical views, etc

INTERNET 2

Brown University

Brown's Judaic Studies dept is hosting a Symposium later this spring.
They have accepted papers from faculty at:

- Duke University
- Hebrew Union College
- University of Edinburgh
- Universität Göttingen
- University of Lausanne
- University of British Columbia
- Collège de France
- Universität Zürich
- Emory University
- Brown University

and want to create a group (in Grouper) that can be used 1) for email communication within this group, and 2) to grant the group members access to a controlled portion of the symposium web site, hosted here at Brown.

Agency/facility/VO collaboration checklist

- Services, and perhaps identity providers, in eduGAIN
- Adhere to federation interop guidelines (e.g. Kantara)
- Move towards an integrated and secure collaboration platform
- Leverages R&S tags for attribute release
- Participates in SIRTIFI trust framework for security
- Moves critical application security to federated MFA
- Promotes ORCID identifiers for researcher identities

- Reasonable to require within N years.